AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

FILED

SEP 25 2015

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

Information associated with staceymonroe2010@yahoo.com, averymonroe1125@yahoo.com and keisha.edwards@yahoo.com that is stored at premises controlled Yahoo, Inc.

Case No. 4:15MJ5474 NAB

APPLICATION FOR A SEARCH WARRANT

I, Jennifer Lynch, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

Information associated with staceymonroe2010@yahoo.com, averymonroe1125@yahoo.com and keisha.edwards@yahoo.com that is stored at premises controlled Yahoo, Inc.

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENTS A and B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18:1591 ; 18:2421 18:1594 ; 18:2422 18:1952	Sex Trafficking by Force,Fraud or Coercion;Transportation of an Individual to Engage in Prostitution, Conspiracy to Commit Sex Trafficking by Force, Fraud or Coercion; Coercion and Enticement to Travel to Engage in Prostitution; Interstate Travel to Promote Prostitution

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Jennifer Lynch
Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: September 25, 2015

Judge's signature

City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge

Printed name and title

AUSA: JENNIFER WINFIELD, 53350MO

AFFIDAVIT

I, Jennifer Lynch, being duly sworn, do hereby depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation and I have worked as such for approximately seven (7) years. My current assignment is with the Public Corruption/Civil Rights Squad where I am detailed to work on various civil rights and human trafficking investigations. I have had numerous contacts and dealings with informants, victims and other individuals known to engage in "prostitution" and sex trafficking related offenses. I also have special training in the area of computer-based investigations. I have investigated and/or assisted in numerous investigations relative to federal cases concerning promoting prostitution and commercial sex-trafficking and related offenses.

2. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Section 1591, which criminalizes sex trafficking by force, fraud or coercion; Title 18, United States Code, Section 1594, which criminalizes conspiracy to commit sex trafficking by force, fraud or coercion; Title 18, United States Code, Section 1952, which criminalizes the act of interstate travel to promote, manage, establish or carry on any unlawful activity, including promoting prostitution; Title 18, United States Code, Section 2421, which criminalizes the transportation of an individual with the intent that the individual engage in prostitution and Title 18, United States Code, Section 2422(a) which criminalizes persuading, inducing, enticing or coercing an individual to travel in

interstate commerce to engage in prostitution. The items that are the subject of the search and seizure applied for in this affidavit are more specifically described in **Attachment A**.

3. I make this affidavit in support of an application for a search warrant for any and all information related to matters involving sex trafficking by force, fraud or coercion, transporting, persuading, inducing, enticing or coercing an individual to travel in interstate commerce to engage in prostitution and interstate travel to promote, manage, establish or carry on any unlawful activity, including promoting prostitution as may be found associated with certain accounts that are stored at the premises owned, maintained, controlled, and/or operated by **Yahoo! Inc.** (hereinafter "**Yahoo**"), an e-mail provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched is described below and in **Attachment A**, attached hereto. This affidavit is made in support of an application for a search warrant under Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **Yahoo** to disclose to the government, records including the contents of communications and other information in its possession pertaining to the subscriber or customer associated with the **Yahoo** email accounts:

i. staceymonroe2010@yahoo.com

ii. averymonroe1125@yahoo.com

iii. keisha.edwards@yahoo.com

Your affiant prepared this affidavit in support of an application for a search warrant because I believe the subject email addresses/accounts contain evidence of violations Title 18, U.S.C. §§ 1591, 1594, 1952, 2421 and 2422(a).

4. The statements contained in this affidavit are based on this affiant's personal knowledge or information provided to this affiant by other law enforcement officers and other agencies. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. Your affiant has set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 1591, 1594, 1952, 2421 and 2422(a) including but not limited to the items described on **Attachment A**, which is attached hereto and incorporated herein by reference.

LOCATIONS TO BE SEARCHED

5. Pursuant to Title 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) your affiant is asking the court to direct **Yahoo** to disclose to the government any and all information in its possession pertaining to the subscriber or customer associated with the following Subject Email Addresses/Accounts: staceymonroe2010@yahoo.com, averymonroe1125@yahoo.com and keisha.edwards@yahoo.com which are maintained by **Yahoo** through its computer systems. These locations are more fully described in **Attachment A**, attached hereto.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 1591, 1594, 1952, 2421 and 2422(a), which criminalize, among other things, transporting, persuading, inducing, enticing or coercing an individual to travel in

interstate commerce to engage in prostitution, sex trafficking by force, fraud or coercion, conspiracy to commit sex trafficking by force, fraud or coercion, as well as interstate travel to promote, manage, establish or carry on any unlawful activity, including promoting prostitution.

7. This Affidavit and Application for Search Warrant seek authorization solely to search the email addresses/accounts and/or files set forth in **Attachment A.**

APPLICABLE LAW ON JURISDICTION

8. This court has authority to issue a search warrant for the records sought by this affidavit even though these records are kept in another District, pursuant to Title 18, United States Code, Section 2703 because, it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

9. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

COMPUTERS, ELECTRONIC COMMUNICATION DEVICES, NEW MEDIA STORAGE DEVICES AND THE CONNECTION TO HUMAN TRAFFICKING:

10. I have investigated matters involving violations of Title 18, United States Code, Sections 1591, 1594, 1952, 2421 and 2422(a). I have been trained regarding the investigation of these types of crimes in which computers are used as a means for receiving, transmitting, and communicating in efforts to exploit victims, as well as services related to human-trafficking, which would include prostitution and other coerced commercial sex services.

11. The development of computers, digital cameras, cellular telephones and the Internet has changed the way in which individuals involved in human-trafficking/prostitution interact with each other. Computers and storage devices for electronic media, cameras and cellular phones serve various functions in connection with human-trafficking/prostitution. They include: (1) advertisement (e.g., via Craigslist.com or Backpage.com); (2) communication (via email, Internet social media, cellular telephone or text) and (3) storage (pictures/images, electronic communications stored on computers, digital cameras and cellular telephones).

12. Human traffickers can now store information and photographs related to their business enterprises on electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMS and DVDs as well as printouts or readouts from any magnetic storage device.

13. Human traffickers and "pimps" can now transfer photographs directly to and from a computer. A device known as a modem permits a computer to connect to other computers through the use of telephone, cable, or wireless connection. Electronic contact can be made to millions of computers around the world. A "pimp" is a term typically used in reference to a man (sometimes a woman), who solicits customers for a prostitute or a brothel, usually in return for a share or all of the earnings that the prostitute makes.

14. The computer's ability to store images (and other electronic data, i.e. emails and other forms of communication) in digital form makes the computer itself an ideal repository for human traffickers and individuals promoting prostitution. The size of the electronic storage media (commonly referred to as the hard drive) used in home

computers has grown tremendously within the last several years. These drives can store hundreds of thousands of pieces of information and images at a very high resolution.

15. The Internet affords individuals interested in human-trafficking/prostitution several different venues for viewing advertisements and communicating relatively anonymously in search for services.

16. Organizers (like pimps) of human-trafficking/prostitution also utilize online resources to send and receive communications via services offered by Internet portals such as **Yahoo** and Hotmail, among others, and social media networking websites like Instagram, Twitter and Tagged.com. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of human-trafficking/prostitution can be found on the user's computer(s). Access to the services can also be done from a cellular telephone (i.e., smart phone, iPhone, etc.).

17. As is the case with most digital technology, communications by way of computer or cellular telephone can be saved or stored on either device which is used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites such as "bookmarked" or "favorite" files. Digital information can also be retained unintentionally, such as traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or internet Service Provider client software, among others). In addition to electronic communications, a computer (and cellular telephone) user's Internet

activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence that shows that a computer contains specific software; when the software was installed; logs regarding the usage of the software; and even some of the files which were uploaded or downloaded using the software. Such information may be maintained indefinitely until overwritten by other data.

BACKGROUND INFORMATION REGARDING COMPUTERS, THE INTERNET AND EMAIL:

18. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as an "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

19. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game counsels and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and

connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

20. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

21. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

22. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

23. "Computer passwords" and "data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

24. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name "www.cybercrime.gov." The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

25. "Internet addresses" take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can be traced to an identifiable physical location and a computer connection. The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.187). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address, it enables Internet sites to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs. There are two types of IP addresses, dynamic and static. To assign dynamic IP addresses, the ISP randomly assigns one of the available IP addresses, in the range of IP addresses controlled by the ISP, each time a customer dials in or connects to the ISP in order to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's dynamic IP address may, and almost always will, differ each time he dials into or connects to the ISP. To assign static IP addresses, the ISP assigns the customer a permanent IP address. The customer's computer would then be configured with this IP address every time he dials in or connects to the ISP in order to connect to the Internet.

26. The "Internet" is a collection of computers and computer networks which are connected to one another via high-speed data links and lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet frequently crosses state and international borders, even if those computers are in the same state. A network is a series of devices, including computers and telecommunication devices, connected by communication channels.

27. An "internet service provider" (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines, ISPs may also provide Internet email accounts and other services unique to each particular ISP such as Usenet Newsgroups and Internet Relay Chat. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, customer service information and other information, both in computer data format and in written record format.

28. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

29. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be

made by any number of means, including modem, local area network, wireless and numerous other methods.

30. Computers connected to the Internet are identified by addresses. Internet addresses take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can identify a physical location and a computer connection.

31. Electronic mail (or "email") is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

Background of Yahoo!, Inc.

32. Based on my training and experience and what I have learned through other sources, I know the following:

a. **Yahoo** provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. **Yahoo** allows subscribers to obtain e-mail accounts at the domain name "**Yahoo**.com," like the email account listed in Attachment A. Subscribers obtain an account by registering with **Yahoo**. During the registration process, **Yahoo** asks subscribers to provide basic personal information. Therefore, the computers of **Yahoo** are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for

Yahoo subscribers) and information concerning subscribers and their use of **Yahoo** services, such as account access information, e-mail transaction information, and account application information.

b. In general, an e-mail that is sent to a **Yahoo** subscriber is stored in the subscriber's "in-box" on **Yahoo** servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on **Yahoo** servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, **Yahoo** and other ISPs have provided their users with larger storage capabilities associated with the user's email account. **Yahoo** and other ISPs have allowed users to store up to ten (10) gigabytes of information associated with the account on ISP servers.

c. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to **Yahoo**'s servers, and then transmitted to its end destination. **Yahoo** often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the **Yahoo** server, the e-mail can remain on the system indefinitely.

d. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by **Yahoo** but may not include all of these categories of data.

e. A **Yahoo** subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files on servers maintained and/or owned by **Yahoo**. Subscribers to **Yahoo** might not store on their home computers copies of the e-mails stored in the **Yahoo** account. This is particularly true when they access their **Yahoo** account through the web, or if they do not wish to maintain particular e-mails or files in their residence. In essence, a subscriber's email box has become a common online data storage location for many users. This is particularly true when they access their **Yahoo** account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

f. In general, e-mail providers like **Yahoo** ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information could include the subscriber's full name, physical address, telephone numbers and other identifiers, such as alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

g. Email providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via **Yahoo**'s website),

and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

h. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications.

i. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

INVESTIGATION

33. During the early morning hours of July 16, 2015, victim "Jane Doe" contacted the 911 dispatch through the St. Louis Metropolitan Police Department after she had just escaped from two suspects who had been forcing her to participate in the commercial sex trade. While speaking with the dispatcher "Jane Doe" was extremely afraid and frantic while hiding behind a dumpster in St. Louis City trying to evade the suspected traffickers. During the phone call "Jane Doe" gave the location of her traffickers as the Westin Hotel,

811 Spruce, Room #359. Following, law enforcement responded to the Westin Hotel and located and detained suspects Thomas Szczerba (hereinafter "SZCZERBA") and Keisha Edwards (hereinafter "EDWARDS").

34. After an interview with victim "Jane Doe" and during the investigation it was determined that approximately 5-6 weeks prior "Jane Doe" had met SZCZERBA and EDWARDS in Houston, Texas. Soon thereafter "Jane Doe" began participating in the commercial sex trade at the direction of SZCZERBA and EDWARDS, ultimately providing all of her earnings to SZCZERBA.

35. From Houston, Texas, SZCERBA transported "Jane Doe" to Chicago, Illinois where they met up with EDWARDS to participate in the commercial sex trade. Following, the three (3) then travelled over the next few weeks within Illinois and then to Wisconsin, and continued participating in the commercial sex trade by utilizing the internet and website postings (including, but not limited to, www.backpage.com and www.eros.com), cellular telephones as well as hotel rooms and condoms. In early July 2015, the three arrived in St. Louis, Missouri and continued their participation in the commercial sex trade.

36. During "Jane Doe's" time with SZCZERBA and EDWARDS, while participating in the commercial sex trade, she was put in a constant state of fear for her safety. "Jane Doe" reported to investigators that SZCZERBA threatened to beat her, had forcefully grabbed her face while yelling and berating her, he had control over her cell phone, and he would deny her requests for food until he decided she could eat and then he would tell her what she could eat. SZCZERBA also would not allow "Jane Doe" to rest until she

reached her daily quota of $1,000 per day, in addition to forcing her to participate in commercial sex dates while she was on her menstrual cycle by using a make-up sponge as a feminine hygiene product. Also, due to the placement of the make-up sponge inside the victim causing severe pain and medical issues, "Jane Doe" subsequently sought medical attention at an area St. Louis hospital. Following, SZCZERBA still required that "Jane Doe" participate in commercial sex activities. Lastly, SZCZERBA gave "Jane Doe" the alias of "Avery Monroe" once she started working for him as a prostitute.

37. During this investigation, your affiant also reviewed numerous subpoenaed records and determined that keisha.edwards@yahoo.com is an email account used to pay for hotel rooms for EDWARDS, SZCZERBA and "Jane Doe." These Hotwire.com and Expedia.com account records detail hotel stays in the areas of St. Louis, Missouri, Wheeling, Illinois, Rosemont, Illinois, Houston, Texas, Wauwatosa, Wisconsin, Washington, D.C., Dallas, Texas, and Waukegan, Illinois.

38. The Expedia.com records show approximately two (2) reservations using the email address keisha.edwards@yahoo.com for June 22, 2015. Also, Hotwire.com records show that from May 27, 2015 through July 15, 2015, there are approximately fourteen (14) reservations using the **Yahoo** email address keisha.edwards@yahoo.com. For example, keisha.edwards@yahoo.com was used to secure a room on July 13, 2015 at The Westin St. Louis, with a payment method of a Bank of America credit card ending in 6506. Even further, records subpoenaed from Bank of America show the same credit card used to secure the reservation at The Westin St. Louis belongs to EDWARDS.

39. The subpoenaed records showed that the prepaid, confirmed Expedia.com and Hotwire.com hotel reservations listed the keisha.edwards@yahoo.com email account and the reservations were often for 1-2 nights. Hotwire.com records show multiple stays in the same city on different days, appearing to be made on a day-to-day basis seeking the lowest rate for the area.

40. The frequency, regularity and length of these prepaid hotel reservations (combined with other information known to investigators), makes these stays consistent with the use of the hotels as a place for illegal commercial-sex transactions. I am aware that such Hotwire.com reservations cannot be made anonymously.

41. Also, based on your affiant's training and experience, I am aware that the adult escort section of www.backpage.com is commonly used by sex workers and pimps to post Internet-based advertisements for thinly-disguised offers of commercial sex. I also know that www.backpage.com requires users to provide an email address in order to list an advertisement. From June 30, 2015 through July 15, 2015, approximately twenty-two (22) adult escort advertisements were posted on www.backpage.com for various cities, to include St. Louis, Missouri, Wauwatosa, Wisconsin, Milwaukee, Wisconsin, and Chicago, Illinois, using email address averymonroe1125@yahoo.com. From November 11, 2012 through May 6, 2015, approximately thirty-four (34) adult section advertisements were posted on www.backpage.com for various cities, to include Phoenix, Arizona, Manhattan, New York, Houston, Texas, Dallas, Texas, and Austin, Texas. For example, the images used in the adult escort advertisements depict both EDWARDS and "Jane Doe" wearing lingerie and posing in sexually suggestive positions. The

advertisements depicting EDWARDS also contained links to EDWARDS' personal erotic webpage, www.staceymonroe.com. The Saint Louis advertisements read as follows and are representative of similar advertisements subpoenaed and reviewed in this case:

> ***Petitte Bombshell Stacey Monroe visiting (last night)!!! – 24, posted July 15, 2015 10:49 PM***
> *Hey guys, I can make your every erotic fantasy come to life!! My insatiable slim petite frame combined with my fun flirty attitude will be sure to put you at ease and keep you coming back again and again. I have a petite but sexy body with subtle curves. My cute smile and bubbly personality will have you longing for more! I'm your sexy and tasteful exotic dream.*
> *Outcalls to surrounding areas. Incall in downtown.*
> *No texts. (260)579-xxxx Stacey Monroe. staceymonroe.com*

> ***Persian/Sicilian Exotic Playmate Visiting last day – Avery Monroe 212-203-5502 – 22, posted July 15, 2015 10:48 PM***
> *Hey guys! I am visiting St. Louis for a few days and I'm looking to spice up my visit. Can you make this night memorable and unforgettable? Seeking mature gentlemen for discreet companionship. Advance notice required. Good hygiene is a must!!*
> *Incall in Downtown Upscale Location. Outcalls to Downtown and surrounding area and surrounding areas.*
> *Serious Inquiries Only. Incall/Outcall 24/7 Avery Monroe 212-203-xxxx*

42. As stated in this affidavit, your affiant is aware that sex traffickers frequently use online providers and email accounts to arrange meetings, transportation and the advertisement of commercial sex because it is fast, readily available and often difficult to trace. I am aware based on my training and experience that certain websites such as www.backpage.com are popular online locations for the promotion of prostitution.

43: Additionally, subpoenaed records show email address staceymonroe2010@yahoo.com was used to establish an account for EDWARDS on the erotic website www.eros.com, which allows users to post advertisements offering sex for

money. In order to establish an account, the user must provide proof of identification showing the user to be of the legal age of 18. EDWARDS provided pictures of 2 driver's licenses from 2 different states. One driver's license was from the state of Nevada and was set to expire August 15, 2016, and the other driver's license was from the state of Texas, with an expiration date of August 15, 2020. In addition to the pictures of the driver's license, EDWARDS submitted a photograph of herself holding a sign stating "Stacey Monroe www.staceymonroe.com 11-11-13". It was determined through the investigation that STACEY MONROE is a known alias for EDWARDS.

44. **Yahoo** email address staceymonroe2010@yahoo.com is listed on the webpage, www.staceymonroe.com, as a contact address for STACEY MONROE, positively identified as EDWARDS. The website, www.staceymonroe.com, is titled "Stacey Monroe, Your Favorite Exotic Playdoll," and advertises various erotic services, such as human toilet, body worship, foot fetish, role play, scissor leg fetish, voyeurism, and light bondage and humiliation. These services are listed under the "menu" section along with various prices, depending on the amount of time an individual wants to spend with STACEY MONROE. The website also contains a "blog" section in which past customers can provide feedback on services, to which STACEY MONROE can reply directly to those customers.

45. Also listed as a form of contact is a link to Twitter account @staceydollxoxo. The Twitter account page contains a link to STACEY MONROE's erotic website, www.staceymonroe.com, and contains a profile picture of an image listed in the "gallery"

section of the erotic website. The Twitter account page has a description of "Your Favorite Exotic Playdoll. Elite companion. Available worldwide by appointment."

46. Also, federal grand jury subpoena requests were sent to **Yahoo** requesting basic subscriber information for the following **Yahoo** email addresses: staceymonroe2010@yahoo.com, averymonroe1125@yahoo.com, and keisha.edwards@yahoo.com. On September 17, 2015, **Yahoo** provided subscriber information for all subject email addresses. The subscriber for **Yahoo** email address averymonroe1125@yahoo.com was listed as Avery Monroe. The subscriber for **Yahoo** email address staceymonroe2010@yahoo.com was listed as Ms. Stacey Monroe. The subscriber for **Yahoo** email address keisha.edwards@yahoo.com was listed as Ms. Keisha Edwards.

47. Your affiant respectfully requests that the affidavit and search warrant be sealed so as not to compromise this on-going investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

48. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require **Yahoo** to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

49. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in control of **Yahoo** there exists evidence of a crime, contraband and/or fruits of a crime. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the **Yahoo** Mail account described in Attachment A was used in criminal activities related to sex trafficking and conspiracy to commit sex trafficking by force, fraud or coercion; interstate travel to promote, manage, establish or carry on prostitution; transportation of an individual with the intent that the individual engage in prostitution and persuading, inducing, enticing or coercing an individual to travel in interstate commerce to engage in prostitution. Accordingly, a search warrant is requested.

50. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST TO SEAL & ORDER NON-DISCLOSURE

52. Because the Investigation is ongoing, I would request the Court to seal the Application for Search Warrant, the Search Warrant, and supporting Affidavit in this matter.

53. Pursuant to 18 U.S.C. § 2705(b), I would request the Court order **Yahoo!**, Inc. not to notify any other person of the existence of this warrant for the next one hundred and eighty (180) days. This request is made because I believe notification of the existence of the warrant will seriously jeopardize the ongoing investigation.

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

This warrant applies to information associated with the **Yahoo! Inc.** e-mail accounts:

i. staceymonroe2010@yahoo.com

ii. averymonroe1125@yahoo.com

iii. keisha.edwards@yahoo.com

which is stored at premises owned, maintained, controlled, or operated by **Yahoo! Inc.**, 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B
Particular Things to be Seized

I. **Information to be disclosed by Yahoo!, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of **Yahoo**, including any messages, records, files, logs, or information that have been deleted but are still available to **Yahoo**, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) made on July 20, 2015 and July 28, 2015, **Yahoo** is required to disclose the following information to the government for each account listed in Attachment A:

a. The contents of all e-mails stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. Any deleted emails, including any information described in subparagraph "a," above;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between **Yahoo**! and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1591, 1594, 1952, 2421 and 2422(a), including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

   a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct;

   b. Any correspondence regarding the solicitation of prostitution or human trafficking by force, fraud or coercion; correspondence pertaining to the persuasion, inducement, and/or enticement of

any individual to engage in any prohibited sexual act or sexual contact; correspondence or the content of the correspondence indicates contact with individuals regarding the solicitation of prostitution or human trafficking by force, fraud or coercion; correspondence between these accounts and any other Facebook accounts where the content of the correspondence discusses solicitation of prostitution or human trafficking by force, fraud or coercion; timeline, wall posts, emails and image files involving the solicitation of prostitution or human trafficking by force, fraud or coercion; files containing visual depictions of individuals engaged in explicit conduct that is commercial in nature;

c. Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts;

d. All correspondence regarding the promotion of prostitution;

e. Any correspondence pertaining to all information related to matters involving sex trafficking by force, fraud or coercion, transporting, persuading, inducing, enticing or coercing an individual to travel in interstate commerce to engage in prostitution and interstate travel to promote, manage, establish or carry on any unlawful activity, including promoting prostitution, including all opened or unopened email;

f. Any email, opened or unopened, where the email address or the content of the email indicates contact with individuals regarding prostitution;

g. Correspondence between these accounts and any other email account where the content of the email discusses all information related to matters involving sex trafficking by force, fraud or coercion, transporting, persuading, inducing, enticing or coercing an individual to travel in interstate commerce to engage in prostitution and interstate travel to promote, manage, establish or carry on any unlawful activity, including promoting prostitution, including all opened and unopened email;

h. Any email, opened or unopened, and any image or video file involving sex trafficking by force, fraud or coercion, transporting, persuading, inducing, enticing or coercing an individual to travel in interstate commerce to engage in prostitution and interstate travel to promote, manage, establish or carry on any unlawful activity, including promoting prostitution, as well as any person engaged in sexually-explicit conduct which is attached to the email;

i. Any file containing visual depictions of persons engaged in sexually-explicit conduct;

j. Any email, opened or unopened, and any image and/or video file that appears to contain passwords or information regarding encryption;

k. Any and all transactional information, to include log files (transmission and usage), of all activity of the accounts, including dates, time, method of connecting, port, dial-up, and/or location, originating Internet Protocol (IP) address, and/or the destination IP address for all opened and unopened email, during the entire period that the account has been active; and

l. Any records of subscriber information, method of payment, or detailed billing.

2. Credit card and other financial information including but not limited to bills and payment records;

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A ;

4. Evidence of the times the account or identifier listed on Attachment A was used;

5. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.

II. By Order of the Court

1. Pursuant to 18 U.S.C. § 2705(b), the Court orders **Yahoo!, Inc.** not to notify any person of the existence of this warrant for one hundred and eighty days (180) days from service of this attachment.